CHAPTER 6

PUBLICATION REQUIREMENTS

A. FEDERAL REGISTER PUBLICATION

1. What must be published in the Federal Register

a. Three types of documents relating to the Privacy Program must be published in the Federal Register:

(1) DoD Component Privacy Program rules;

(2) Component exemption rules; and

(3) System notices.

b. See DoD 5025.1-M (reference (o)) and DoD Directive 5400.9 (reference (P)) for information pertaining to the preparation of documents for publication in the Federal Register.

2. The effect of publication in the Federal Register

Publication of a document in the Federal Register constitutes official public notice of the existence and content of the document.

3. DoD Component rules

a. Component Privacy Program procedures and Component exemption rules are subject to the rulemaking procedures prescribed in reference (p).

b. System notices are not subject to formal rulemaking and are published in the Federal Register as "Notices," not rules.

c. Privacy procedural and exemption rules are incorporated automatically into the Code of Federal Regulations (CFR). System notices are not published in the CFR.

4. Submission of rules for publication

a. Submit to the Defense Privacy Office, ODASD(A), all proposed rules implementing this Regulation in proper format (see references (o) and (p)) for publication in the Federal Register.

b. This Regulation has been published as a final rule in the Federal Register. Therefore, incorporate it into your Component rules by reference rather than by republication (see reference (p)).

c. DoD Component rules that simply implement this Regulation need only be published as final rules in the Federal Register (see references (o) and (p)).

d. Amendments to Component rules are submitted like the basic rules.

e. The Defense Privacy Office submits the rules and amendments thereto to the Federal Register for publication.

5. Submission of exemption rules for publication

a. No system of records within the Department of Defense shall be considered exempt from any provision of this Regulation until the exemption and the exemption rule for the system has been published as a final rule in the Federal Register (see subsection A.3. of this Chapter).

b. Submit exemption rules in proper format to the Defense Privacy Office. After review, the Defense Privacy Office will submit the rules to the Federal Register for publication.

c. Exemption rules require publication both as proposed rules and final rules (see DoD Directive 5400.9, reference (p)).

d. Section B. of this Chapter discusses the content of an exemption rule.

e. Submit amendments to exemption rules in the same manner used for establishing these rules.

6. Submission of system notices for publication

a. While system notices are not subject to formal rulemaking procedures, advance public notice must be given before a Component may begin to collect personal information or use a new system of records. The notice procedures require that:

(1) The system notice describes the contents of the record system and the routine uses for which the information in the system may be released.

(2) The public be given 30 days to comment on any proposed routine uses before implementation; and

(3) The notice contain the date on which the system will become effective.

c. Submit system notices to the Defense Privacy Office in the Federal Register format (see reference (p) and Appendix E). The Defense Privacy Office transmits the notices to the Federal Register for publication.

d. Section C. of this Chapter discusses the specific elements required in a system notice.

B. EXEMPTION RULES

1. General procedures. Subsection 2a. of Chapter 5 provides the general guidance for establishing exemptions for systems of records.

2. Contents of exemption rules

a. Each exemption rule submitted for publication must contain the following:

(1) The record system identification and title of the system for which the exemption is claimed (see subsections C.2. and C.3. of this Chapter);

(2) The specific subsection of the Privacy Act under which exemptions for the system are claimed (for example, 5 U.S.C. 552a(j)(2), 5 U.S.C. 552a(k)"(3); or5 U.S.C. 552a(k)(7);

(3) The specific provisions and subsections of the Privacy Act from which the system is to be exempted (for example, 5 U.S.C. 552a(c)(3), or 5 U.S.C. 552a(d)(l)-(5)) (see Appendix D); and

(4) The specific reasons why an exemption is being claimed from each subsection of the Act identified.

b. Do not claim an" exemption for classified material for individual systems of records, since the blanket exemption applies (see subsection A.3. of Chapter 5).

C. SYSTEM NOTICES

1. Contents of the system notices

a. The following data captions are included in each system notice:

(1) Systems identification (see subsection C.2. of this Chapter).

(2) System name (see subsection C.3. of this Chapter).

(3) System location (see subsection C.4. of this Chapter).

(4) Categories of individuals coveredby the system (see subsection C.5. of this Chapter).

(5) Categories of records in the system (see subsection C.6. of this Chapter).

(6) Authority for maintenance of the system (see subsection C.7 of this Chapter).

(7) Purpose(s) (see subsection C.8. of this Chapter).

(8) Routine uses of records maintained in the system, including categories of users, uses, and purposes of such uses (see subsection C.8. of this-Chapter).

(9) Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system (see subsection C.9. of this Chapter).

(10) Systems manager(s) and address (see subsection C.1O. of this Chapter)

(11) Notification procedure (see subsection C.11. of this Chapter).

(12) 'Record access procedures (see subsection C.12. of this Chapter).

(13) Contesting records procedures (see subsection C.13. of this Chapter)

(14) Record source categories (see subsection C.14. of this Chapter)

(15) Systems exempted from certainprovision of the Act (see subsection C.15. of this Chapter).

b. The captions listed in paragraph C. la. of this Chapter have been mandated by the Office of Federal Register and must be used exactly as presented.

c. A sample system notice is shown in Appendix E.

2. System identification. The system identifier must appear on all system notices and is limited to 21 positions, including Component code, file number and symbols, punctuation, and spacing.

3. System name

a. The name of the system reasonably identifies the general purpose of the system and, if possible, the general categories of individuals involved.

b. Use acronyms only parenthetically following the title or any portion thereof, such as, "Joint Uniform Military Pay System (JUMPS)." Do not use acronyms that are not commonly known unless they are preceded by an explanation.

c. The system name may not exceed 55 character positions including punctuation and spacing.

4. System location

a. For systems maintained in a single location provide the exact office name, organizational identity, and address or routing symbol.

b. For geographically or organizationally decentralized systems, specify each level of organization or element that maintains a segment of the system.

c. For automated data systems with a central computer facility and input/output terminals at several geographically separated locations, list each location by category.

d. When multiple locations are identified by type of organization, the system location may indicate that official mailing addresses are contained in an address directory published as an appendix to the Component system notices in the Federal Register. Information concerning format requirements for

preparation of an address directory may be obtained from the project officer, Air Force Data Services Center (AFDSC/GNM), Washington, DC 20330.

e. If no address directory is used or the addresses in the directory are incomplete, the address of each location where a segment of the record system is maintained must appear under the "System Location" caption.

f. Classified addresses are not listed, but the fact that they are classified is indicated.

g. Use the standard U.S. Postal Service two letter state abbreviation symbols and zip codes for all domestic addresses.

5. Categories of individuals covered by the system

a. Set forth the specific categories of individuals to whom records in the system pertain in clear, easily understood, nontechnical terms.

b. Avoid the use of broad over-general descriptions, such as "all Army personnel" or "all ❑ ilitary personnel" unless this actually reflects the category of individuals involved.

6. Categories of records in the system

a. Describe in clear, nontechnical terms the types of records maintained in the system.

b. Only documents actually retained in the system of records shall be described, not source documents that are used only to collect data and then destroyed.

7. Authority for maintenance of the system

a. Cite the specific provision of the federal statute or Executive Order that authorizes the maintenance of the system.

b. Include with citations for statutes the popular names, when appropriate (for example, Title 51, United States Code, Section 2103, "Tea-Tasters Licensing Act"), and for Executive Orders, the official title (for example, Executive Order No. 9397, "Numbering System for Federal Accounts Relating to Individual Persons").

cm Cite the statute or Executive Order establishing the Component for administrative housekeeping records.

d. If the Component is chartered by a DoD Directive, cite that Directive as well as the Secretary of Defense authority to issue the Directive. For example, "Pursuant to the authority contained in the National Security Act of 1947, as amended (10 U.S.C. 133d), the Secretary of Defense has issued DoD Directive 5105.21, the charter of the Defense Intelligence Agency (DIA) as a separate Agency of the Department of Defense under his control. Therein, the Director, DIA, is charged with the responsibility of maintaining all necessary and appropriate records."

8. Purpose *or* Purposes

a. List the specific purposes for maintaining the system of records by the Component.

b. Include the uses made of the information within the Component and the Department of Defense (so-called "internal routine uses").

9. Routine uses

a. The blanket routine uses (Appendix C) that appear at the beginning of each Component compilation apply to all systems notices unless the individual system notice specifically states that one or more of them do not apply to the system. List the blanket routine uses at the beginning of the Component listing of system notices (see paragraph B.6.d. of Chapter 4).

b. For all other routine uses, when practical, list the specific activity to which the record may be released, to include any routine automated system interface (for example, "to the Department of Justice, Civil Rights Compliance Division," "to the Veterans Administration, Office of Disability Benefits," or "to state and local health agencies").

c. For each routine user identified, include a statement as to the purpose or purposes for which the record is to be released to that activity (see subsection B.5. of Chapter ,4).

d. Do not use general statements, such as, "to other federal agencies as required" or "to any other appropriate federal agency."

10. Policies and practices for storing, retiring, accessing, retaining, and disposing of records.

This caption is subdivided into four parts:

a. Storage. Indicate the medium in which the records are maintained. (For example, a system may be "automated, maintained on magnetic tapes or disks," "manual, maintained in paper files," or "hybrid, maintained in a combination of paper and automated form.") Storage does not refer to the container or facility in which the records are kept.

b. Retrievability. Specify how the records are retrieved (for example, name and SSN, name, SSN) and indicate whether a manual or computerized index is required to retrieve individual records.

c. Safeguards. List the categories of Component personnel having immediate access and those responsible for safeguarding the records from unauthorized access. Generally identify the system safeguards (such as storage in safes, vaults, locked cabinets or rooms, use of guards, visitor registers, personnel screening, or computer "fail-safe" systems software). Do not describe safeguards in such detail as to compromise system security.

d. Retention and Disposal. Indicate how long the record is retained. When appropriate, also state the length of time the records are maintained by the Component, when they are transferred to a Federal Records Center, length

of retention at the Records Center and when they are transferred to the National Archivist or are destroyed. A reference to a Component regulation without further detailed information is insufficient.

11. System manager or managers and address

a. List the title and address of the official responsible for the management of the system.

b. If the title of the specific official is unknown, such as for a local system, specify the local commander or office head as the systems manager.

c. For geographically separated or organizationally decentralized activities for which individuals may deal directly with officials at each location in exercising their rights, list the position or duty title of each category of officials responsible for the system or a segment thereof.

d. Do not include business or duty addresses if they are listed in the Component address directory.

12. Notification procedures

a. If the record system has been exempted from subsection (e)(4)(G) of the Privacy Act (reference (b)) (see subsection A.4. of Chapter 5), so indicate.

b. For all nonexempt systems, describe how an individual may determine if there are records pertaining to him or her in the system. The procedural rules may be cited, but include a brief procedural description of the needed data. Provide sufficient information in the notice to allow an individual to exercise his or her rights without referral to the formal rules.

c. As a minimum, the caption shall include:

(1) The official title (normally the system manager) and official address to which the request is to be directed;

(2) The specific information required to determine if there is a record of the individual in the system.

(3) Identification of the offices through which the individual may obtain access; and

(4) A description of any proof of identity required (see subsection A.3. of Chapter 3).

d. When appropriate, the individual may be referred to a Component official who shall provide this data to him or her.

13. Record access procedures

a. If the record system has been exempted from subsection (e)(4)(H) of reference (b) (see subsection A.4. of Chapter 5), so indicate.

b. For all nonexempt records systems, describe the procedures under which individuals may obtain access to the records pertaining to them in the system.

c. When appropriate, the individual may be referred to the system manager or Component offical to obtain access procedures.

d. Do not repeat the addresses listed in the Component address directory but refer the individual to that directory.

14. Contesting record procedures

a. If the record system has been exempted from subsection (e)(4)(H) of the Privacy Act (reference (b)) (see subsection A.4. of Chapter 5), so indicate.

b. For all nonexempt systems of records, state briefly how an individual may contest the content of a record pertaining to him or her in the system.

c. The detailed procedures for contesting record accuracy, refusal of access or amendment, or initial review and appeal need not be included if they are readily available elsewhere and can be referred to by the public. (For example, "The Defense Mapping Agency rules for contesting contents and for appealing initial determinations are contained in DMA Instruction 5400.11 (32 CFR Part 295c.")

d. The individual may also be referred to the system manager to determine these procedures.

15. Record source categories

a. If the record system has been exempted from subsection (e)(4)(I) of reference (b) (see subsection A.4. of Chapter 5), so indicate.

b. For all nonexempt systems of records, list the sources of the information in the system.

c. Specific individuals or institutions need not be identified by name, particularly if these sources have been granted confidentiality (see subsection C.2. of Chapter 5).

16. System exempted from certain provisions of the Act

a. If no exemption has been claimed for the system, indicate "None."

b. If there is an exemption claimed indicate specifically under which subsection of reference (b) it is claimed.

c. Cite the regulation and CFR section containing the exemption rule for the system. (For example, "Parts of this record system may be exempt under Title 5, United States Code, Sections 552a(k)(2) and (5), as applicable. See exemption rules contained in Army Regulation 340-21 (32 CFR Part 505).")

17. Maintaining the master DoD system notice registry

a. The Defense Privacy Office maintains a master registry of all DoD record systems notices.

b. Coordinate with the Defense Privacy Office to ensure that all new systems are added to the master registry and all amendments and alterations are incorporated into the master registry.

D. NEW AND ALTERED RECORD SYSTEMS

1. Criteria for a new record system

a. A new system of records is one for which there has been no system notice published in the Federal Register.

b. If a notice for a system of records has been canceled or deleted before reinstating or reusing the system, a new system notice must be published in the Federal Register.

2. Criteria for an altered record system. A system is considered altered whenever one of the following actions occurs or is proposed:

a. A significant increase or change in the number or type of individuals about whom records are maintained.

(1) Only changes that alter significantly the character and purpose of the record system are considered alterations.

(2) Increases in numbers of individuals due to normal growth are not considered alterations unless they truly alter the character and purpose of the system;

(3) Increases that change significantly the scope of population covered (for example, expansion of a system of records covering a single command's enlisted personnel to include all of the Component’s enlisted personnel would be considered an alteration).

(4) A reduction in the number of individuals covered is not an alteration, but only an amendment (see subsection El. of this Chapter).

(5) All changes that add new categories of individuals to system coverage require a change to the “Categories of individuals covered by the system” caption of the notice (subsection C.5. of this Chapter) and may require changes to the “Purpose(s)” caption (subsection C.8. of this Chapter).

b. An expansion in the types or categories of information maintained.

(1) The addition of any new category of records not described under the “Categories of Records in System” caption is considered an alteration.

(2) Adding a new data element which is clearly within the scope of the categories of records described in the existing notice is an amendment (see subsection El. of this Chapter).

(3) All changes under this criterion require a change to the "Categories of Records in System" caption of the notice (see subsection c.6. of this Chapter).

c. An alteration in the manner in which the records are organized or the manner in which the records are indexed *and retrieved.*

(1) The change must alter the nature of use or scope of the records involved (for example, combining records systems in a reorganization).

(2) Any change under this criteria requires a change in the "Retrievability" caption of the system notice (see paragraph C.10.b. of this Chapter).

(3) If the records are no longer retrieved by name or personal identifier cancel the system notice (see subsection Al. of Chapter 1).

d. A change in the purpose for which the information in the system is used.

(1) The new purpose must not be compatible with the existing purposes for which the system is maintained or a use that would not reasonably be expected to be an alteration.

(2) If the use is compatible and reasonably expected, there is no change in purpose and no alteration occurs.

(3) Any change under this criterion requires a change in the "Purpose(s)" caption (see subsection C.8. of this Chapter) and may require a change in the "Authority for maintenance of the system" caption (see subsection C.7. of this Chapter);

e. Changes that alter the computer environment (such as changes to equipment configuration, software, or procedures) so as to create the potential for greater or easier access.

(1) Increasing the number of offices with direct access is an alteration.

(2) *Software releases,* such as operating systems and system utilities that provide for easier access are considered alterations.

(3) The addition of an on-line capability to a previously batch-oriented system is an alteration.

(4) The addition of peripheral devices such as tape devices, disk devices, card readers, printers, and similar devices to an existing ADP system constitute an amendment if system security is preserved (see subsection El. of this Chapter).

(5) Changes to existing equipment configuration with on-line capability need not be considered alterations to the system if:

(a) The change does not alter the present security posture; or

(b) The addition of terminals does not extend the capacity of the current operating system and existing security is preserved;

(6) The connecting of two or more formerly independent automated systems or networks together creating a potential for greater access is an alteration.

(7) Any change under this caption requires a change to the "Storage" caption element of the systems notice (see paragraph C.10.a. of this Chapter).

3. Reports of new and altered systems

a. Submit a report of a new or altered system to the Defense Privacy Office before collecting information for or using a new system or altering an existing system (see Appendix F and subsection D.4. of this Chapter).

b. The Defense Privacy Office coordinates all reports of new and altered systems with the Office of the Assistant Secretary of Defense (Legislative Affairs) and the Office of the General Counsel, Department of Defense.

c. The Defense Privacy Office prepares for the DASD(A)'s approval and signature the transmittal letters sent to OMB and Congress (see subsection D.5. of this Chapter).

4. Time restrictions on the operation of a new or altered system

a. All time periods begin from the date the DASD(A) signs the transmittal letters (see paragraph D.3.c. of this Chapter). The specific time limits are:

(1) 60 days must elapse before data collection forms *or* formal instructions pertaining to the system may be issued.

(2) 60 days must elapse before the system may become operational; (that is, collecting, maintaining, using, or disseminating records from the system) (see also subsection A.6. of this Chapter).

(3) 60 days must elapse before any public issuance of a Request for Proposal or Invitation to Bid for a new ADP or telecommunication system. (NOTE: Requests for delegation of procurement authority may be submitted to the General Services Administration during the 60 days' waiting period, but these shall include language that the Privacy Act reporting criteria have been reviewed and that a system report is required for such procurement.)

(4) Normally 30 days must elapse before publication in the Federal Register of the notice of a new *or* altered system (see subsection A.6. of this Chapter) and the preamble to the Federal Register notice must reflect the date the transmittal letters to OMB and Congress were signed by DASD(A).

b. Do not operate a system of records until the waiting periods have expired (see section D. of Chapter 10).

5. Outside review of new and altered systems reports. If no objections are received within 30 days of a submission to the President of the Senate, Speaker of the House of Representatives, and the Director, OMB, of a new or altered system report it is presumed that the new or 'altered systems have been approved as submitted.

6. Exemptions for new systems

See subsection A.5. of this Chapter for the procedures to follow in submitting exemption rules for a new system of records.

7. Waiver of time restrictions

a. The OMB may authorize a federal agency to begin operation of a system of records before the expiration of time limits set forth in subsection D.4. of this Chapter.

b. When seeking such a waiver, include in the letter of transmittal to the Defense Privacy Office an explanation why a delay of 60 days in establishing the system of records would not be in the public interest. The transmittal must include:

(1) How the public interest will be affected adversely if the established time limits are followed; and

(2) Why earlier notice was not provided.

c. When appropriate, the DefensePrivacy Office shall contact OMB and attempt to obtain the *waiver.*

(1) If a waiver is granted, the Defense Privacy Office shall notify the subcommittee and submit the new or altered system notice along with any applicable procedural or exemption rules for publication in the Federal Register.

(2) If the waiver is disapproved, the Defense Privacy Office shall process the system the same as any other new or altered system and notify the subcommittee of the OMB decision.

d. Under no circumstances shall the routine uses for new or altered system be implemented before 30 days have elapsed after publication of the system notice containing the routine uses in the Federal Register. This period camot be waived.

E. AMENDMENT AND DELETION OF SYSTEMS NOTICES

1. Criteria for an amended system notice

a. Certain minor changes to published systems notices are considered amendments and not alterations (see subsection D.2. of this Chapter).

b. Amendments do not require a report of an altered system (see subsection D.3. of this Chapter), but must be published in the Federal Register.

2. System notices for amended systems. When submitting an amendment for a system notice for publication in the Federal Register include:

a. The system identification and name (see subsections C.2. and C.3. of this Chapter).

b. A description of the nature and specific changes proposed.

c. The full text of the system notice is not required if the master registry contains a current system notice for the system (see subsection C.17. of this Chapter).

3. Deletion of system notices

a. Whenever a system is discontinued, combined into another system, or determined no longer to be subject to this Regulation, a deletion notice is required.

b. The notice of deletion shall include:

(1) The system identification and name.

(2) The reason for the deletion.

c. When the system is eliminated through combination or merger, identify the successor system or systems in the deletion notice.

4. Submission of amendments and deletions for publication

a. Submit amendments and deletions to the Defense Privacy Office for transmittal to the Federal Register for publication.

b. Include in the submission at least one original (not a reproduced copy) in proper Federal Register format (see Appendix G).

c. Multiple deletions and amendments may be combined into a single submission.